A Report to COTS by the Privacy, Security & Access Work Group

Toward the Use of Digital Signatures in the Commonwealth of Virginia

October 27, 1999

Dear Colleague:

The Council on Technology Services (COTS) was established in August 1998 by Governor Jim Gilmore under the Chairmanship of Secretary of Technology Donald Upson. In November of 1998, several COTS work groups were designated to explore and address a variety of technology issues which most affect the quality, convenience and efficiency of service delivery by Virginia government. Among these was the Privacy, Security and Access (PSA) work group.

In initial meetings, the PSA work group grappled with scope and mission, identifying a broad and comprehensive array of pertinent issues. A PSA Web site intended to serve as a resource on these topics for the Commonwealth technology community was constructed and now may be visited at http://state.vipnet.org/cts/index.html.

Following discussion at a COTS meeting in late May, the issue of digital signatures for the Commonwealth was identified as a priority for the work group. (*Digital* signatures are an important and distinctive subset of the family of *electronic* signatures.) Between June and October the work group has researched and dialogued with local, state, federal and industry colleagues about digital signatures and Public Key Infrastructures (PKI), the complex framework of legal, policy, operational and technical issues within which digital signatures operate.

Over the five month period, the work group has met in monthly sessions, sponsored an educational overview on digital signatures to COTS, hosted a panel at the Commonwealth of Virginia Information Technology Symposium (COVITS), monitored legislative developments at the state and federal levels, conducted a video teleconference at the Department of Information Technology to confer with colleagues in the State of Washington, held a strategy session at the Dept. of Game & Inland Fisheries on potential "first wave" deployments and participated in a session hosted by the University of Virginia to explore architectural alternatives.

In mid-September, the work group was apprised of the issuance of Executive Order 51(99), which provides the following:

> **I.** The Secretary of Technology, with the assistance of DIT, DTP, andVIPNet, shall review available alternatives and recommend a plan to facilitate the use and authentication of electronic signatures by both the private andpublic sectors in the Commonwealth. This plan shall be submitted to the Governor no later than November 1, 1999.
>
> **J.** Agencies and institutions shall follow the Secretary of Technology's guidance in incorporating into their proposed plans for Web-enabled government the use of electronic signature technology for boththeir internal and external transactions.

This report is intended to inform Secretary Upson and COTS of key findings about the use and deployment of digital signatures. The report offers a strategy to enable the Commonwealth to meet the objectives of:

- assuming leadership in developing and widely deploying this important technology, and
- hastening realization of the benefits it provides to promote a robust and secure environment in which efficient and convenient e-government can flourish.

Sincerely,

Cheryl Clark, Chair

COTS Privacy, Security and Access Work Group

cc: The Honorable Donald W. Upson

Privacy, Security, and Access Work Group Members
Council of Technology Services

CHAIRPERSON

Cheryl F. Clark, CIO
Senior Commissioner for Technology
Department Motor Vehicles

MEMBERS

Jim Adams
Information Technology Manager
Department of Information Technology

Ray Davis
Director of Administration/CFO
Department of Game & Inland Fisheries

Dan Galloway
Deputy Information Technology Director
State Corporation Commission

Darrell L. Gasaway
Information Services Director
Department of Juvenile Justice

Carrie Gillotte
Director of Application Systems
George Mason University

Patricia Jackson
Director, Information Systems External Programs
Virginia Polytechnic Institute

Margaret Maupin
Director, Management Audit & Review Services
Department of General Services

Ed Morris
Deputy Director
Department of Corrections

Mike O'Neil
Deputy Commissioner for Finance & Administrations
Department of Social Services

John Palese
Information Security Manager
Department of Social Services

Andy Poarch (Ex Officio member)
Executive Director of the
Virginia Council on Technology Services

Bill Russell
Deputy Director
County of Chesterfield

Teresa Thomas
Office of the Auditor of Public Accounts

Captain R. Lewis Vass
Criminal Justice Information Systems
Virginia State Police

Daniel D. Ziomek
Policy & Planning Specialist
Department of Technology Planning

STAFF

Kevin Cadieux
Vivian Cheatham

CONTRIBUTORS

Janet Arnold
Health Canada

Gerry Anderson
Regional Management State & Local Government Sales
Entrust Technologies

Leslie Carter
Deputy Director of Services
Department of Information Technology

Claudine Conway
Strategic Account Manager
GTSI

Mark Davis
Territory Manager
Network Associates, Inc.

Sally Fehn
Applications Development Manager
Unisys Corporation

Chip German
Director of Policy & Planning
University of Virginia

Richard Guida
Chairman, Federal PKI Steering Committee

Dan Houlihan
General Manager
Virginia Interactive, LLC

Virgil Kopf
CIO for Information Management Services
Department of Game & Inland Fisheries

Tom Littauer
Senior Consultant
Amdahl Corporation

David Molchany
Chief Information Officer
County of Fairfax

Fred Norman
Client Business Director
Unisys Corporation

John Pfeiffer
Specialist
Network Associates, Inc.

Rama Ramanathan
Advanced Security Technology
Unisys

Murali Rao
Director, Data Management Division
Virginia Department of Transportation

George Riesco
Nexus

Dennis Reynolds
Government Relations Manager
Entrust

Kevin Scully
CEO
WebCritical Technologies

Tim Sigmon
Director, Advanced Technology
University of Virginia

Prasanna Simha
Sales Executive - EMS
Computer Associates

Jerry Simonoff
Director
Department of Technology Planning

Mike Thomas
Deputy Secretary of Technology
Department of Information Technology

John Westrick
Assistant Attorney General
Office of the Attorney General

Brandon Weidner
Sales Executive - EMS
Computer Associates

The COTS Privacy, Security, and Access Work Group gratefully acknowledges those government agencies and industry advisors who contributed to the knowledge represented in this report.

Center for Excellence in Government
Computer Associates
County of Chesterfield
County of Fairfax
Department of Corrections, Commonwealth of Virginia
Department of Game and Inland Fisheries, Commonwealth of Virginia
Department of General Services, Commonwealth of Virginia
Department of Information Services, State of Washington
Department of Information Technology, Commonwealth of Virginia
Department of Juvenile Justice, Commonwealth of Virginia
Department of Motor Vehicles, Commonwealth of Virginia
Department of Social Services, Commonwealth of Virginia
Department of State Police, Commonwealth of Virginia
Department of Technology Planning, Commonwealth of Virginia
Department of Transportation, Commonwealth of Virginia
Entrust Technologies
Federal PKI Steering Committee
GTSI
Health Canada
Network Associates, Inc.
Nexus
Office of the Attorney General, Commonwealth of Virginia
Office of the Auditor of Public Accounts, Commonwealth of Virginia
State Corporation Commission, Commonwealth of Virginia
Unisys Corporation
University of Virginia
Virginia Interactive, LLC
Virginia Polytechnic Institute
WebCritical Technologies

A special acknowledgment of gratitude is extended to DMV Commissioner Richard D. Holcomb for providing staff, facilities and special services to assist in producing this report.

I. Executive Summary

Three decades ago, a new world of electronic communication called the Internet appeared on the horizon. Today, this new electronic world is no longer a thin line in the distance; it is enveloping and changing the way in which business is conducted, the method in which people communicate with each other, and the manner in which relationships are formed. With the same rapid pace, more information and transactions are being transmitted over the Internet, exposing the need for increased security. Security is critical because it provides the technologies, policies, and infrastructure that permit E-business transactions between parties (who may not have a pre-existing relationship) to occur with the assurance that the parties are who they claim to be, and that the contents of the transaction have not been altered or intercepted.

Security technology performs several functions in E-business transactions: access control, authentication, confidentiality, data integrity, and technical non-repudiation. Digital signatures, through the use of a public key infrastructure (PKI), are designed to solve the problem of trustworthiness using a Certification Authority to provide authentication as a trusted third party. The benefits of implementing the use of digital signatures via a PKI solution have yielded tangible results ranging from validation and approval of invoice payments to reducing the turnaround time of standardized forms.

Both state and federal entities have been at the forefront in incorporating security measures into their Internet policies and procedures. As with all issues, the struggle between balancing the decentralization of control and mandating sufficient regulation to maintain trust and safety for constituents is a primary concern for all government entities. Several state and federal agencies have taken the initiative to tackle these concerns and have successfully implemented pilot programs for digital signatures through the use of a PKI. Valuable lessons learned are already being modeled from these programs as the use of digital signatures and PKI continues to be explored as the solution for Internet communication and transaction security.

Given Virginia's ranking as the "Internet Capitol of the World", the Commonwealth is in an opportune position to provide leadership in establishing model digital signature and PKI policies and programs. As the state of Virginia begins its efforts to create new ways of conducting business safely over the Internet, legal issues must be addressed to promote and support the transition to e-government.

Summary of Recommendations

Recommendation 1: PKI and digital signature technology are key elements of a robust e-commerce environment and the Commonwealth must quickly embrace this technology in order to advance E-commerce and economic growth.

Recommendation 2: Recommend action in the 2000 Virginia General Assembly.

Recommendation 3: Develop a Commonwealth Bridge Certificate Architecture (CBCA).

Recommendation 4: Commission "first wave" deployments.

Recommendation 5: Designate governance for the Commonwealth's Digital Signature Initiative, including establishment of a new COTS Work Group, separate from the PSA Work Group.

Recommendation 6: Designate interim certificate authorities & associated services.

Recommendation 7: Provide seed money from the Technology Infrastructure Fund.

II. Introduction

Computers are radically changing the way that citizens, businesses, and governments interact. More than 50 million Americans now have access to the Internet, and estimates of online purchases during 1998 ranged between $8 billion and $13 billion. American businesses have sustained the longest period of uninterrupted growth in their history with much of it being attributed to the new efficiencies made possible by process reengineering that leverages the Internet. As more transactions take place over computer networks, and as the meaning of the phrase "computer network" grows from a workgroup to include the Internet, an electronic means to authenticate business transactions and make legal, binding commitments is needed. An alternative to the familiar handwritten signature and some means to securely transmit sensitive information over public networks are required. Electronic signatures and electronic authentication are the means to make business over the Internet a safe and trusted process.

States have been leaders in the effort to establish the laws, regulations, and policies that make electronic authentication possible. To date, forty-four states have passed laws or regulations recognizing some form of electronic signature as valid. State officials are working together to develop electronic authentication systems that are compatible across multiple jurisdictions. The federal government also plans to adopt standards this year to accept electronic signatures in federal government transactions. These standards are intended to be consistent with existing state policies. (1)

The Internet is the very centerpiece of the global information evolution and Virginia is the Internet capital of the world. In addition to being the birthplace of the Internet, almost half of the Internet backbone is in Virginia and companies located in the Commonwealth serve nearly half of all online service subscribers. Accordingly, it is appropriate that Virginia take a leadership role in establishing model policies that will empower her citizens to reap the full benefits of this technology in the workplace, in the classroom, and for personal use. (2)

The explosive advent of the Internet has challenged many fundamental assumptions regarding communications and commerce, perhaps none as greatly as security. Its openness makes it the ideal platform for global commerce and communications and the Internet offers the promise of inexpensive mass communication and provides economies of scale for low-cost distribution. But, the Internet's fundamental strength, its openness, is also its weakness. Since it is open, communications are inherently difficult to secure. What is missing is the mechanism to guarantee the integrity of information and provide relationships of trust that are the foundations of a commercial infrastructure. The Internet's economic potential will not be fully realized until service providers can deliver a guaranteed measure of security for mission-critical and large-scale commercial applications. (3)

The elements of a secure business environment are access control (also referred to as "authorization"), authentication, confidentiality, data integrity, and technical non-repudiation (see Exhibit 1). Each is a necessary component for a complete solution. Access is typically managed by the application using PKI tools. A firewall, which regulates data flow into and out of a network, may be compared to a lock on the door. While vital, it can prevent business as well as securing it. This is the reason for the more fine-grained security made possible by PKI. Authentication binds the identity of an individual to a specific message or transaction. For commercial or legal use, authentication must be as legally acceptable as a signature on a contract. Confidentiality and data integrity ensure that communications and transactions remain confidential and unaltered. Legal and commercial applications often demand privacy, not merely as a preference but as a legal prerequisite. Data integrity assures that information remains accurate and is not altered. This requires a practical method to validate data after transmission or storage. Non-repudiation prevents reneging on an agreement by denying participation in a transaction. Public key technology provides mechanisms that address each of these requirements. (4)

Digital Signatures, through the use of PKI technology, are an essential component of a trusted, robust E-commerce environment. It is the public key infrastructure that will serve as the means of assuring security and trust on the Internet, ultimately unleashing its economic potential. Effective security creates an environment that facilitates electronic commerce and private communications. This means not only creating a climate that is safe from robbery and fraud, but more importantly, a place where business agreements can be transacted under commonly accepted legal standards.(5)

Exhibit 1
Fundamental Security Requirements
(Source: Governnment Information Technology Services Board)

Authentication	Ensure that transmissions and messages, and their originators, are authentic, and that a recipient is eligible to receive specific categories of information.
Confidentiality	Ensure that information can be read only by authorized entities.
Data Integrity	Ensure that data is unchanged from its source and has not been accidentally or maliciously altered.
Non-Repudiation	Ensure strong and substantial evidence is available to the sender of data that the data has been delivered (with the cooperation of the recipient) and, to the recipient, of the sender's identity, sufficient to prevent either from successfully denying having sent or received the data. This includes the ability of a third party to verify the integrity and origin of the data.

The 1998 FBI/Computer Security Institute survey found that 72% of security breaches resulted in financial loss. Although survey respondents reported net losses greater than $136 million, the actual dollar value of losses from specific information security breaches is difficult to estimate and is under-reported since companies are reluctant to admit compromise or loss due to concerns regarding client trust. (6) It should be noted that state government's primary security risk categories, unauthorized insider access and theft of proprietary information, are ranked one and two in the table below.

Exhibit 2

The Average Loss of Various Security Attacks

Type of Attack	Average Financial Loss ($)
Unauthorized Insider Access	$2,809,000
Theft of Proprietary Information	$1,677,000
Telecom Fraud	$539,000
Financial Fraud	$388,000
Sabotage	$86,000
System Penetration by Outsider	$86,000

Source: 1998/CSI/FBI Computer Crime & Security Survey

In any exchange of important information, each party needs to be confident about the other's identity. This confidence traditionally is achieved using handwritten signatures and government-issued identification such as passports or driver's licenses. Without the ability to authenticate another person's identity, it is impossible to enter into binding contracts or reliably transfer confidential information. Electronic commerce and electronic government are enhanced by reliable and legally enforceable electronic authentication systems. When combined with other important components of an electronic transaction infrastructure, such as methods to ensure data integrity and confidentiality, electronic authentication helps establish the framework to do business in the twenty-first century.

Governors can support state leadership in electronic authentication by:

- encouraging the acceptance of electronic authentication by state agencies;
- ensuring that state electronic authentication standards allow a wide variety of technologies and experimentation;
- participating in state-led efforts to develop electronic authentication systems that are compatible across jurisdictions; and
- participating in the development of electronic authentication standards for use by the federal government. (7)

III. Electronic Signatures and their Components

The Nature of Signatures

A written signature commonly serves one or more of the following purposes:

- **identification of a person**
- **verification of the party creating or sending the record**
- **verification of the informational integrity of the record**
- **verification of a party's authority**
- **acknowledgment of receipt.**

Electronic signatures, though different in form, will serve the same purposes. Further, electronic signatures may include the execution of a process. What is critical in all cases is that execution or adoption is conducted with the "intent to sign". (1)

Legal Signatures and Electronic Signatures

The American Bar Association (ABA) defines a "legal signature" as having the following characteristics:

> **Signer authentication**: To provide good evidence of *who participated* in a transaction, a signature should indicate by whom a document or message is signed and be difficult for any other person to produce without authorization.
> **Document authentication**: To provide good evidence of the *substance* of the transaction, a signature should identify what is signed, and make it impracticable to falsify or alter, without detection, either the signed matter or the signature.
> **Affirmative act**: To serve the *ceremonial and approval functions* of a signature, a person should be able to create a signature to mark an event, indicate approval and authorization, and establish the sense of having legally consummated a transaction.
> **Efficiency**: Optimally, a signature and its creation and verification processes should provide the *greatest* possible assurance of authenticity and validity with the *least* possible expenditure of resources. (2)

On October 20, 1998, President Bill Clinton signed the Government Paperwork Elimination Act (GPEA) as part of H.R. 4328, the Fiscal 1999 Omnibus Appropriations Act. GPEA instructs the National Technology and Information Administration (NTIA) and the Office of Management and Budget (OMB) to develop electronic signature standards for use by federal agencies by May 2000. The act requires the electronic signature to identify and authenticate a particular person and indicate that person's approval of the message content, but does not specify a particular technology for use in the standards. GPEA also

includes a provision that electronic records and electronic signatures are not to be denied legal effect, enforceability, or validity simply because they are in electronic form rather than on paper. The standards are to be developed in consultation with appropriate state and industry standards-setting bodies and must:

- be compatible with existing state and industry standards;
- not inappropriately favor one industry or technology;
- be as reliable as appropriate for the purpose in question;
- keep the information submitted intact;
- provide for electronic acknowledgement of the submission; and provide multiple authentication methods for any form that would result in 50,000 or more submittals. (3)

The GPEA defines "electronic signature" as a method of signing an electronic message that (A) identifies and authenticates a particular person as the source of the electronic message; and (B) indicates such person's approval of the information contained in the electronic message. (GPEA, section 1709(1)).

This definition should be interpreted by reference to accepted legal definitions of signatures. The term "signature" has long been understood as including "any symbol executed or adopted by a party with *present intention to authenticate a writing*." (Uniform Commercial Code, 1-201(39)1970)).

The Code of Virginia, Section 59.1-467, defines an “electronic signature” as “...any electronic identifier intended by the person making, executing, or adopting it to authenticate and validate a record.”

It is extremely important to understand the practical distinction between “electronic” and “digital” signatures. In practice, digital signatures are a *subset* of the family of electronic signatures, which may include such things as PIN numbers, *digitized* signatures and other forms of biometrics.

Digital signatures, uniquely, have the following set of characteristics. The signature is:

a. unique to the signer
b. capable of verification
c. under the signer’s sole control
d. linked to the record in such a manner that it can be determined if any data contained in the record was changed subsequent to the electronic signature being affixed to the record
e. and created by a method appropriately reliable for the purpose for which the electronic signature was used. (4)

Public Key Infrastructures

Digital signatures operate within a framework of hardware, software, policies, people and processes referred to as a public key infrastructure (PKI).

Public key infrastructures are based on principles associated with public key cryptography. Public key cryptography encrypts information by using two mathematically related keys: one is kept private; the other is made public. The private key cannot be determined from the public key. An individual who wants, for example, to send a message uses his or her private key of the recipient to encrypt the message. The recipient uses his or her public key to decrypt the message. The sender therefore knows that only the intended recipient can read the message. (5)

A PKI is a system that provides the basis for establishing and maintaining a trustworthy networking environment through the generation and distribution of keys and certificates. It may be established as either "managed" or "unmanaged".

A **"managed"** PKI is a comprehensive system that provides a completely trusted networking environment for E-business through best of breed security, flexibility, and ease of use. A managed PKI provides the following capabilities automatically and transparently to the user:

- Certificate authority
- Registration authority
- Non-repudiation
- Cross certification with other certificate authorities
- Key backup and recovery
- Management of key histories
- Timestamping
- Certificate revocation
- Automatic key update
- Seamless support of all secured applications

An **"unmanaged"** PKI is a certificate-generating system only. The above bullet points are not part of the unmanaged infrastructure. It is a Certificate Authority only, enabling users to use certificates for authentication to applications. Security of those applications is application-dependent in an unmanaged solution, as opposed to being managed completely by the PKI in the managed solution. (6)

Trust Model and Certificate Authority

Third Party Trust

Third-party trust refers to a situation in which two individuals trust each other even though they have not previously established a personal relationship. In this situation, two individuals trust each other because they each share a relationship with a common third party, and that third party vouches for the trustworthiness of the two people.

Third-party trust is a fundamental requirement for any *large-scale* implementation of a network security product based on public-key cryptography. Public-key cryptography requires access to users' public keys. In a large-scale network, however, it is impractical and unrealistic to expect each user to have previously established relationships with all other users. In addition, because users' public keys must be widely available, the association between a public key and a person must be guaranteed by a trusted third party to prevent masquerading. In effect, users trust any public key certified by the third party because they trust that organization to operate the third-party certification agent in a secure manner. (7)

Registration Authority

The registration authority (RA) refers to the people, processes, and tools used to support the registration of users within the PKI and ongoing administration, most importantly the revocation of certificates. The designated RA is responsible and liable for accurately authenticating certificate authority users. The certificate authority relies on the RA for instruction as to whom it should grant a digital certificate.

Certificate Authority

Certificate authorities (CA) hold a central role in the PKI by acting as the repository of trust from which digital certificates derive legitimacy. Digital certificates are created, managed, administrated, and revoked by the CA. Much like the government which issues and guarantees the identity of the passport bearer, a CA acts as the guarantor of the validity of the digital certificate. By electronically signing a digital certificate, a CA vouches for the certificate owner's identity. The main function of a digital certificate is to validate the public key of an individual or network device (e.g., to validate content). However, digital certificates can also contain information that defines user privileges, and therefore they can play a role in managing access control. (8) Specifically, they contain the information about the individual that the CA is willing to vouch for. In the case of a passport agency that is citizenship and date of birth. Every CA will likely have different information specific to the enterprise and to the individual's role in the enterprise.

The portability and scalability of a digital certificate supports a wide variety of applications. For example, digital certificates and private encryption keys can be loaded onto smart cards. Over time, digital certificate-configured smart cards will likely become the standard for credentials such as passports, driver's licenses, and credit cards. (9)

Both a passport issuing office and a certification authority combine policies with physical elements. In the case of the passport office, there is a set of policies determined by the government dictating which people are deemed to be citizens and the process through which citizens may obtain a passport. Business managers within an organization, acting as the RA, determine security policies and decide which people in the organization can be issued digital certificates and associated privileges. (10) An organization's PKI is governed by a set of policy rules contained in the "certificate policy" while the organization's CA grants digital certificates according to the organization's "certificate practice statement" or CPS.

From a physical perspective, a passport office can be looked upon as the creator of secure, authorized paper documents. The passport office has special equipment to securely bind together information on a citizen (name, picture, date of birth, etc.) in such a way that it is extremely difficult to alter the passport without detection. Consequently, someone examining a passport is assured that the passport has integrity. While the passport office has physical equipment to create secure paper documents, a CA has a computing platform and electronic cryptographic keys that are used to create and verify secure electronic identities for network users. Specifically, the CA creates electronic "certificates," the authenticity and integrity of which is guaranteed through a digital signature created by the CA's signing private key. Users verify the CA's signature on certificates by using the CA's verification public key. (11)

The passport office must protect physical access to its passport generation equipment to guarantee the authenticity of passports; similarly, access to the CA's signing private key must be carefully protected and granted only to highly trusted individuals within the CA domain. (12)

Before proceeding to a discussion of certificates, there is one additional network security trust concept that benefits from the passport office analogy. The concept is that of a "CA domain." The term CA domain refers to the population of users for which the CA has the authority to issue certificates (e.g., Commonwealth of Virginia constituents, agency employees, etc.). This is analogous to a passport office because one country does not have the right to issue passports for citizens of another country. The domain of a passport office is restricted solely to citizens of its own country. (13)

Digital Certificates

Digital certificates provide a registered identity to users to assure other parties with whom they communicate that they are "safe." Safe communication occurs when identities of

communicating parties are proven valid and trustworthy. These identities are proven trustworthy since the certificate authority (the agent of trust in the PKI) signs the digital certificates before issuing them. That signature's validity is verified with each usage of the certificate. Digital certificates are stored as a “public key certificate” using a standard X.509 v3 format. This format is an industry-accepted standard. Certificates are created after the Certificate Authority signs a set of data, which includes the following:

1. The user's name in the format of a distinguished name (DN). The DN specifies the user's name and any additional attributes required to uniquely identify the user.
2. A public key of the user. The public key is required so that others can encrypt for the user or verify the user's digital signature.
3. The validity period, or lifetime of the certificate (a start date and an end date).
4. The specific operations for which the public key is to be used. (whether for encrypting data (i.e. secure email), verifying digital signatures, or both). (14)

Digital Signature Technology

Digital signature technology uses a mathematical process known as public key cryptography to provide electronic authentication. Cryptography uses very large numbers, known as encryption keys, to scramble the data in a transmission. In order to use a digital signature, there must be two related encryption keys. The private key is used to encrypt the transmission and must be kept confidential. The public key is used to decrypt the transmission when it is received and must be freely available to others. Because only the public key can decrypt data encrypted with its related private key, the data receiver can be sure that the private key owner originally sent the data. (15)

Digital signatures generally do not encrypt the actual data sent in a transmission. Instead, they encrypt a smaller version of the data known as a message digest. The message digest is created in such a way that if any part of the original data is changed, a different message digest will be produced. Then the message digest is encrypted using the private key and sent along with the original data. Because encrypting large files either takes a very powerful computer or a long time, message digests allow digital signatures to provide effective authentication without overwhelming computer resources. Message digests also provide proof that data has not been altered in transit. If the message digest generated from the received file is the same as the decrypted digital signature, then the data is exactly the same as originally sent. (16)

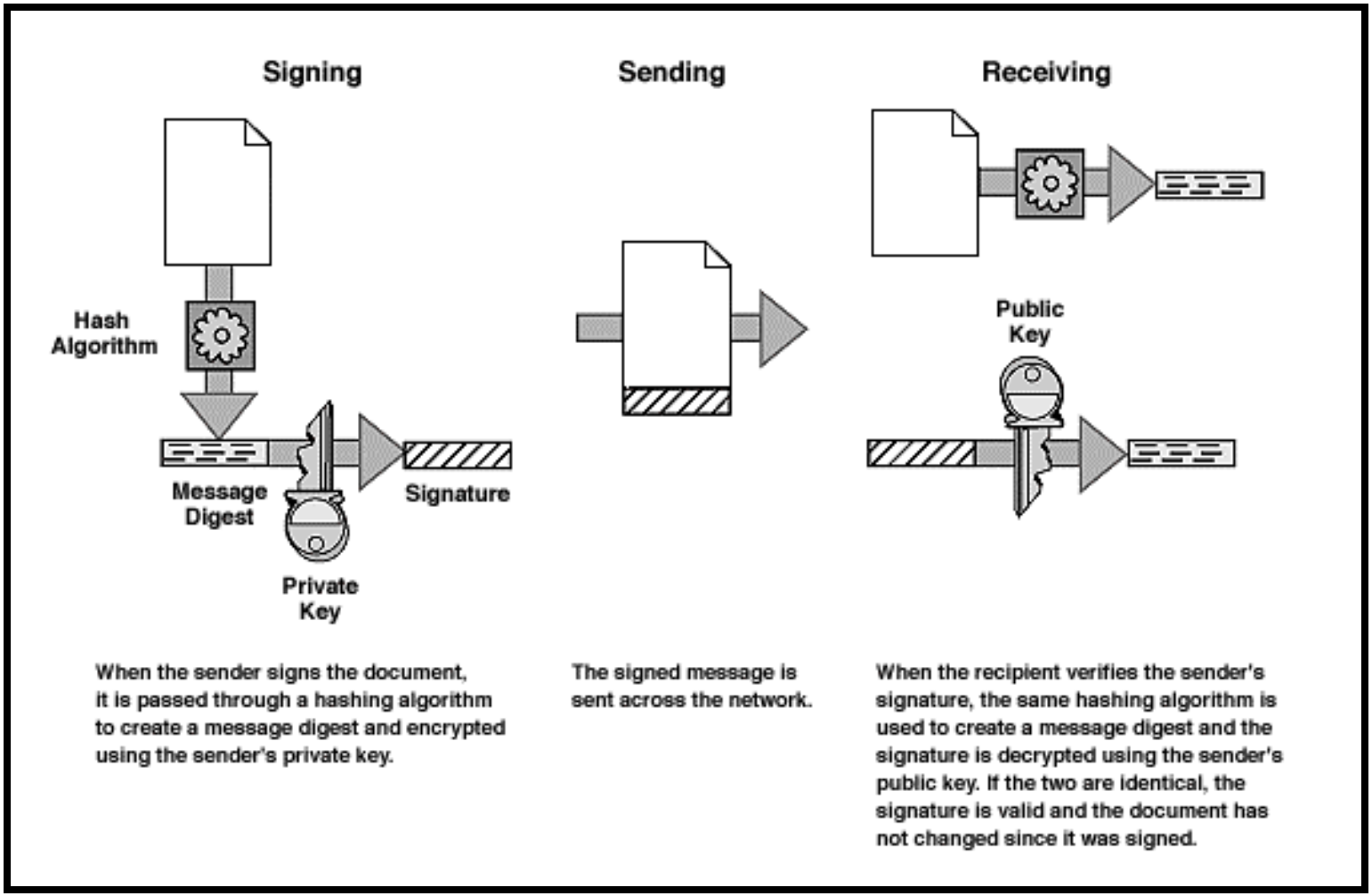

Exhibit 3
Source: Hambrecht & Quist

System Integrity

The integrity of a digital signature system depends on three factors. The first is an unbreakable private key. It must be impossible to derive the private key from the public key, or anyone could gain access to the private key. As long as the digital signature is based on an encryption system that has been thoroughly tested and is generally accepted by the cryptographic community, then sufficient safeguards will exist to prevent breaking the private key. The second factor is the system for issuing and maintaining the encryption keys. This system is based on certification authorities (CA) as previously discussed. (17) The third factor is the education of users of the system that they must **never** allow anyone else to know the private key. Anyone who knows the private key has, in effect, a full unlimited power of attorney to act for the user.

Summation

Digital signature systems provide a detailed framework for electronic authentication. They address most questions about the requirements for acceptable electronic authentication, and, if the public/private keys are managed properly, they provide a very high level of certainty as to the identity of the signer of a transmission. Digital signature technology also ensures that the transmission has not been altered in transit, something that is not usually provided by other types of electronic authentication.

IV. Legal Frameworks

Legality of Digital Signatures

The concept of the signature has been in existence since humans began to write. The definitional characteristics of a signature exist in the legal world as well as the electronic world. The American Bar Association has put the concept of ***digital*** signatures, a subset of electronic signatures, to their "legal signature" definition and has stated that the processes of creating a digital signature and verifying it accomplish the essential *effects* desired of a signature as defined below:

Signer authentication: If a public and private key pair is associated with an identified signer, the digital signature attributes the message to the signer. The digital signature cannot be forged, unless the signer loses control of the private key (a "compromise" of the private key such as by divulging it or its associated personal identification number (PIN) or pass phrase or by losing the media device in which it is contained.
Message authentication: The digital signature also identifies the signed message, typically with far greater certainty and precision than paper signatures. Verification reveals any tampering, since the comparison of the hash results (one made at signing and the other made at verifying) shows whether the message is the same as when signed.
Affirmative act: Creating a digital signature requires the signer to use the signer's private key. This act can perform the "ceremonial" function of alerting the signer to the fact that the signer is consummating a transaction with legal consequences. (It is noted that if the person "signing" the message is not a human being but a device under the control of a human being, the ceremonial function *may* be undermined.)
Efficiency: The processes of creating and verifying a digital signature provide a high level of assurance that the digital signature is genuinely the signer's. They can be set up to run with great speed and accuracy, with human interaction only for non-routine processing decisions. Compared to paper methods such as checking bank signature cards and other methods so tedious and labor-intensive that they are rarely used, digital signatures yield a high degree of assurance without adding greatly to the resources required for processing. (1)

Virginia's Legal Framework

There is a significant and growing level of legislative activity underway at both the federal and state levels concerning the use of digital signatures in traditional governmental business practices. Currently, the Code of Virginia (Sections 1-13.32, 2.1-7.4 and 59.1-467 through 59.1-469) provides a minimally sufficient basis for State agencies and institutions to use "electronic" signatures. However, 59.1-469 further defines and authorizes State officials to use "electronic" signatures only when they meet five specific criteria.

"The Electronic Signature is:

a. unique to the signer
b. capable of verification
c. under the signer's sole control
d. linked to the record in such a manner that it can be determined if any data contained in the record was changed subsequent to the electronic signature being affixed to the record
e. and created by a method appropriately reliable for the purpose for which the electronic signature was used." (2)

Arguably, *only* digital signatures, made possible through a PKI, can meet all five criteria. If the Commonwealth can use only those electronic signatures which meet all five criteria, this could have the unfortunate consequence of constraining all electronic signatures to one choice, a PKI-enabled digital signature. Because digital signatures are the most binding and authenticated subset of electronic signatures, they may be excessive for many Commonwealth functions. These functions can be satisfied by alternative signing methods that are much simpler, less costly, and more readily available.

Therefore, legislation should be proposed to the 2000 General Assembly with a two-fold objective:

a. to maintain a legal framework minimally sufficient to enable public sector use of digital signatures, in accordance with guidelines and criteria developed at the direction of the Secretary of Technology, and

b. not to preclude the use of other appropriately valid forms of electronic signatures, in addition to digital signatures, many of which are already in use throughout the Commonwealth today.

These changes are necessary to enable and promote a smooth and cost-effective transition to electronic transactions, to eliminate the pervasive confusion between electronic and digital signatures, and to establish uniform enterprise criteria for their appropriate use. Agencies should apply guidelines and criteria issued at the direction of the Secretary of Technology, on a case by case basis, to the legal and operational characteristics of individual business functions and services to determine which electronic signing techniques are most appropriate to specific Commonwealth functions and services.

V. Digital signature use within the Commonwealth and other States

Virginia Department of Game and Inland Fisheries

In August of this year, the Department of Game and Inland Fisheries (DGIF) became the first among Virginia's public sector organizations to deploy digital signatures. The application, using products and services from Entrust and Shana Corporations, involves more than sixty internal forms. Benefits include elimination of paper, elimination of redundant handling and associated errors, improved productivity and turnaround, and better security.

In the future, DGIF intends to move boating registration renewals to the web, to implement secure e-mail, and to use virtual private networking technology to extend services to field personnel. Potentially, this will reduce costs for the agency, increase efficiencies and provide a trusted enterprise network.

More information can be found in the Appendix to this report.

State of Washington Case Study

The State of Washington, in preparation for drafting and release of its RFP for PKI services, initiated two pilots in which digital signatures were utilized as a business enabler. These policy initiatives were intended to be short duration projects whose purpose was to discover as many issues as possible (i.e. policy, legal, financial, cultural, and technical) that acted as impediments to PKI implementation. The office of Strategic Initiatives, an office of the Department of Information Services, sought out agencies willing to learn about PKI and who had a business process where a transaction occurred that would benefit from reengineering using digital signatures. Washington identified two business processes in which to pilot its PKI: invoice processing in the state motor pool and individual retirement form submission within the Department of Retirement Services.

The first of these pilots involved a process in which three or more signatures, culminating in the accounting department, were required to validate and approve an invoice for payment from the motor pool all the way into the state's accounting general ledger system. This process used a non-electronic method of signing and transportation and could take as long as 30 days, thus incurring a late payment penalty. With the introduction of digital signatures, the same form could be signed, verified that the signer was valid and had not changed the document's content three separate times in the course of an hour. The form was then electronically converted and automatically entered into Washington's General Ledger accounting computer system for immediate payment. This enabled employees to process an exponentially larger number of invoices as well as take advantage of early payment discounts. Notice that while PKI was valuable and will likely

avoid duplication in future security-conscious applications, a new application and new procedures had to be built.

The second pilot allowed the Department of Retirement Services to create a "smart" form enabling its members to change their personal information in the Department's systems. The "smart" form allows automated rules to be set within the form that forces the user to fill it out correctly the first time. The employee then digitally signs the form and submits it directly to the Department's information systems thus negating the need to be reentered by Department of Retirement Services personnel. This reengineered process not only eradicated a time intensive manual process but it drastically reduced the "per transaction" cost of creating and transporting forms and the amount of labor required to process the forms. The Department thus successfully reduced an eight -step process to three steps and increased its customers' satisfaction levels by a factor of two. Cost savings were also achieved with the ability to post one form on the Internet for all employees to download that was at once current, as well as accessible, statewide for the one time development cost of the form.

The State of Washington's pilot experiences have been an invaluable resource in terms of lessons learned. Among these are:

- Agencies should focus on automating routine, high volume, low value business routines. This reduces the cost-per-transaction and provides the greatest efficiencies

- Not all business processes or transactions are appropriate candidates for PKI reengineering with digital signatures.

- Involve stakeholders in designing process and they will embrace it. The process change must be perceived as a benefit to ALL process users or it will not be adopted.

- Be prepared to evolve your digital signature-enabled process over time to ensure best of breed solution with 100% stakeholder adoption.

- Allow users authentication and certificate registration with a minimum amount of cost and intrusion, thus ensuring that users are insulated from the technical aspects of the certificate registration process (cryptology, key technology, etc.)

- Provide an easy to use, transparent, and seamless digital signature-enabled application for the end user to reduce technical frustration and time-consuming non-productive process activities.

- Provide a quick, cost-effective approach for the creation of new electronic business processes that replace paper-based methods between multiple entities. Allow staff to implement "their" ideas.

- Allow digital signatures to be integrated easily into a large number of email, electronic forms, and common office applications (i.e. documents, spreadsheets, etc.). Leverage the systems you already have in place.

- Provide an attractive "per subscriber" cost that is better than current multiple username/password business solutions.

- Use of "smart" electronic forms drastically reduces the amount of error correction time required by users.

- Do not mandate workflow steps. Users understand best the next level of action that is required in their business workflow. Allow them to direct the form to the next logical individual for action.

- Convey to agencies/users that this will be a long-term solution that will be supported over a long period; thus, justifying their investment in time and money to implement a PKI solution.

- The benefits of digital signatures are not always apparent up front. The technology and workflow paradigm shifts are so new as to cause hesitation in acceptance. If a PKI is provided that is adequately explained and incorporates user input, employees will embrace the new process.

- Ensure that the entire business lifecycle of the transaction is taken into account from inception through its archival requirements.

- Involve state auditing agencies early, as they will become strong allies in helping to identify deficiencies in transaction lifecycle management practices.

VI. A Course of Action for the Commonwealth

Pace of Adoption of Digital Signatures and PKI's

While PKI's and digital signature technologies are not new, adoption to this point has been slow. Deployments have generally been limited in size and scope due to legal uncertainties, costs, complexity, evolution of standards and immaturity of the technology itself. In the near term, deployments will multiply at both the federal and state levels and demand will grow for the increased security, convenience and potential savings digital signature capabilities afford.

In the public sector, federal agencies represent the greatest number of deployments within an enterprise as well those which are largest in scale. Use will continue to grow in the near term and scale of use will accelerate. Richard Guida, Chairman of the Federal PKI Steering Committee, stated in his remarks at the COVIT Symposium that during 2000 the following four agencies will expand the number of active certificates they have issued from around 1000 each to the following:

Federal Aviation Administration to over 20,000
Federal Deposit Insurance Corporation to over 7,000
National Aeronautics & Space Administration to over 25,000
Department of Energy to over 20,000.

The Department of Defense, which has issued about 50,000 certificates, is expected to have over 4 million certificates in use by 2002.

A handful of states have conducted pilots and have relatively small scale deployments in pilot or early production mode. Several states including Washington, Illinois, Texas and New York currently have RFP's pending to acquire PKI products and services at the enterprise level, although no state has a production enterprise solution.

According to a forecast in materials distributed by the Gartner Group at the Symposium ITxpo99, 80% of large enterprises will conduct one or more pilots between 1999 and 2003.

Assuming a Leadership Position

If immediate action is undertaken, the Commonwealth would be in a good position to assume a leadership role in adoption of PKI and digital signatures at the enterprise level.

Experiences and products of other states, the federal government and concerned organizations are abundant. These include Certificate policies, Certificate Practice Statements, guidelines, standards, lessons learned, business case models, architecture and

trust models, actual and model statutes, etc. Selectively, these can be adapted to fit the needs of the Commonwealth and leveraged to gain position and momentum.

First Wave Demonstration Initiatives

The following agencies and local governments have been identified as candidates to pursue a "f*irst wave*" of demonstrations:

- Department of Game & Inland Fisheries
- Department of Information Technology
- Department of Motor Vehicles
- Department of Transportation
- Chesterfield and Fairfax Counties.

The First Wave initiatives would demonstrate use of digital signatures in these categories: transactions internal to an agency, agency to agency exchanges (with some level of applications integration), agency to business partners, and agency to local governments. It would be highly desirable to demonstrate a government to *citizen* exchange as well.

Candidate functions include:

- Internal forms
- Forms transferred between agencies
- Service or purchase documents between agency and business partners
- Contracts between agency and business partners
- Certification of collections between agency and local governments
- Secure and signed e-mail.

Certificate Authorities (CA)

As part of the demonstrations, the Commonwealth will need to have a CA to administer and manage certificates for the participating agencies. The Department of Information Technology will establish a memorandum of understanding with the subcontractor for the Virginia Interactive Providers Network (VIPnet) to act as a temporary CA for the period of the demonstration. The Department of Game and Inland Fisheries, which already serves as its own CA, will serve as a second CA for participating organizations.

Bridging Certificate Authorities

In parallel and in full collaboration with these efforts, the University of Virginia will develop a bridge certification architecture for use by the Commonwealth based on a model under construction at the federal level.

The Commonwealth's bridge certification architecture (CBCA) will provide the capability of cross-certifying between different CA's. The CBCA will give organizations a practical choice whether to operate under the Commonwealth's enterprise CA (with the administrative advantages and economies of scale this will offer) or under a different CA which may be more suitable to that organization's business functions.

The CBCA will also position the Commonwealth advantageously to face issues related to interoperating with CA's across jurisdictional lines. This is an issue which will grow in scope and urgency as more the number of CA's continues to grow.

The question of whether to have a purely hierarchical model with a single CA or a web model with multiple CA's is typically posed for an "either-or" response. By taking the two pronged approach of developing in parallel a bridge certification architecture in collaboration with an enterprise architecture, the Commonwealth will demonstrate foresight, leadership and assume a position which is both flexible and adaptable to a variety of business models and missions. It is potentially establishes the best of both worlds.

Timing and Results

To prepare for statutory and funding issues which may need to be addressed in the 2001 session of the General Assembly, the demonstrations will need to begin immediately and conclude in the early fall of 2000.

Successful completion of the effort should result in the following:

- The foundation of policies, practices, guidelines and standards necessary to transition into an enterprise production environment
- An enterprise technical architecture and acquisition strategy based on experience
- A Commonwealth Bridge Certification Architecture
- An invested knowledge and skills base for decision makers and technical staff
- A demonstrated working solution of trust and confidence extensible to the Commonwealth public sector community, to business partners and to the public.

VII. Findings and Recommendations

Recommendation 1: PKI and digital signature technology are key elements of a robust e-commerce environment and the Commonwealth must quickly embrace this technology in order to advance e-commerce and economic growth.

The PKI is best thought of as a framework of accepted business practices and legal statutes supported by systems and software. Writing code and building systems is easy; the difficult part is establishing new business practices and consumer behaviors. The rate of change in human behavior will ultimately define the rate at which the PKI is accepted. However, we believe acceptance is inevitable because of PKI's superiority in securing communications, validating identity, and confirming transactions when compared to legacy business practices. (1) By many measures, the PKI provides mechanisms for establishing trust and binding commitments that are superior to accepted business practices. Electronic commerce tools based on public key technology will substitute for and eventually replace established "commerce archetypes" such as paper contracts, personal signatures, and currency. (2) In the meantime, as we make this e-transition, various forms of electronic signatures will exist with digital signatures being the most binding, non-reputable, and secure.

Recommendation 2: Recommend Virginia legislation and a supporting resolution

Legislation is recommended for the 2000 session of the General Assembly to enable agencies to adopt electronic signatures, including the subset designated as *digital* signatures. (See section IV above for more detail.)

The Secretary of Technology, working with the Council on Technology Services, should submit to the General Assembly for its consideration a resolution that would support the policy direction and principles that the Secretary is following to promote the utilization of digital signatures in the Commonwealth as a means of fostering electronic business.

Legislative activity is intense in both the federal and state arenas. It is essential that the Commonwealth continue to monitor and actively assess the implications of federal and state legal and legislative developments for potential adoption within Virginia. It will be highly desirable for demonstration efforts and associated policy development activities to be completed by the early fall of 2000 in order to finalize any actions to be recommended to the 2001 General Assembly.

Recommendation 3: Develop bridge architecture for certificate authorities

Efforts should be endorsed by the University of Virginia to guide development of a bridge certification architecture based on the federal model for use by the Commonwealth. The bridge will give organizations a practical choice whether to operate under the Commonwealth's Enterprise Certificate Authority or a different certificate authority.

This would be done in parallel and in collaboration with proposed "first wave" deployments and with the associated development of legal, administrative and operational policy frameworks.

Recommendation 4: Commission "first wave" deployments

The following four agencies, two local governments, and VIPnet have volunteered to pursue potential first wave deployments in a coordinated effort between now and early fall of 2000:

The Department of Game & Inland Fisheries
The Department of Information Technology
The Department of Motor Vehicles
The Department of Transportation
Chesterfield and Fairfax Counties

Other agencies or organizations should be invited to join in the pilot demonstrations by providing the Secretary of Technology with a statement of intent and description of the proposed demonstration within thirty days from the delivery of this report to COTS. Reference Section VI for more details about the potential demonstrations.

In order to meet this schedule, the plan must be commissioned and adequate resources assigned immediately.

Recommendation 5: Establish a separate workgroup, in addition to PSA, to guide development of the Commonwealth's Digital Signature Initiative.

A new COTS workgroup should be established to proceed with enabling PKI/digital signatures as guided by the findings and recommendations in this report. Membership in this group should leverage the considerable knowledge acquired and working relationships established in the process of developing this report. Members should include the pilot agencies and localities (DGIF, DMV, VDOT, DIT, Chesterfield and Fairfax Counties), the University of Virginia, and VIPnet.

Additional members should be appointed to the work group from the Office of the Attorney General, Department of Accounts, Department of General Services, Office of the Auditor of Public Accounts, and the Department of Information Technology. These individuals will be instrumental in addressing associated legal and administrative issues and in co-authoring a Commonwealth Certification Policy and Certification Practices Statement, in collaboration with other work group members.

In order to expedite this effort and make it successful, a qualified, full-time project manager and senior level staff should be assigned to support and assist the COTS work group to achieve its mission.

The Governor should appoint members to a oversight committee to steer and support the working groups. The oversight committee should be chaired by the Secretary of Technology.

Industry partners have been essential and invaluable contributors in the creation of this report and should continue to be an integral part of the process going forward.

The Privacy, Security & Access workgroup, from which this initiative emerged, should continue to pursue its broader mission, including articulation of a security architecture for the Commonwealth and in support of points E and F in Executive Order 51 (99).

Recommendation 6: Designate interim certificate authorities & associated services

DGIF currently has the capability to act as a certificate authority and has agreed to provide this service on a limited basis for the duration of the demonstrations.

VIPnet should be designated to act as a second certificate authority and provide associated services for the "first wave" deployments. The Department of Information Technology should enter into a memorandum of understanding with the subcontractor who operates VIPnet to establish the scope, duration, terms and conditions necessary for this arrangement.

Registration Authority services should be conducted by the individual agencies/organizations for their own employees and for any of their business partner participants.

Recommendation 7: Provide seed money

The Secretary of Technology should make disbursements in fiscal year 2000, of a total amount not to exceed $100,000, from the Technology Infrastructure Fund to serve as seed money to further the Commonwealth's digital signatures initiative. The Secretary should consult with the Council on Technology Services and the Digital Signatures Steering Committee in making these disbursements.

VIII. Glossary of Terms

Certificate Authorities

The Certification Authority (CA) is the system responsible for issuing secure electronic identities to users in the form of certificates. In creating certificates, CA's act as agents of trust in a PKI, by signing the digital certificates. This signature on a certificate ensures that any tampering with the contents of the certificate can be easily

detected. As long as users trust a CA and its business policies for issuing and managing certificates, they can trust certificates issued by the CA.

Certificate Policy

A named set of rules that indicates the applicability of a certificate to a particular community and or class of application with common security requirements. It indicates whether or not the public key certificate in question is suitable for a particular application or purpose. A Certification Authority may adopt more than one Certificate Policy, but in each case, the document serves as the cornerstone of establishing trust in a public key certificate, and it constitutes a basis for cross-certification.

Certificate Practice Statement (CPS)

A comprehensive description of how all policy requirements stated in the Certificate Policy will be implemented and maintained by a Certification Authority.

A Certification Authority with a single CPS can support more than one confidentiality Certificate Policy and more than one digital signature Certificate Policy. A number of Certification Authorities that do not have identical CPS' may support the same Certificate Policy.

Confidentiality

The assurance that information is not disclosed to inappropriate entities or processes.

Certificate Revocation

To permanently end the operational period of a certificate from a specified time forward.

Cross-Certification

Cross-certification is a process in which two CA's securely exchange keying information so that each can effectively certify the trustworthiness of the other's keys. Essentially, cross-certification is simply an extended form of third-party trust in which network users in one CA domain implicitly trust users in all other CA domains which are cross-certified with their own CA.

Digital Certificates

Digital Certificates provide a registered identity to users to insure that other parties with whom they communicate are “safe.” Safe communication occurs when identities of communicating parties are proven valid and trustworthy. These identities are proven trustworthy since the Certificate Authority (the agent of trust in the PKI) signs the digital certificates before issuing them. That signature's validity is verified with each usage of the certificate.

Directory Services

Directory Services are necessary for the functioning of a Public Key Infrastructure (PKI). The Directory holds the user's certificates, which contain their public keys. Also, the Directory contains the list of revoked certificates (CRL lists). The Directory is an important piece of the PKI infrastructure, as it is accessed frequently for the following purposes:

- Public keys stored in the certificates on the directory are accessed to allow users to be able to decrypt encrypted messages, which have been sent encrypted to ensure confidentiality.
- Public keys are also accessed to verify digital signatures applied to authenticate the sender.
- Public keys ensure that interaction with users whose certificates have been revoked does not occur.

The Directory should utilize the LDAP (Lightweight Directory Access Protocol) standard. For implementations involving chaining of multiple directories, or replication of a directory, it should also be an X.500 directory in addition to LDAP.

Digital Signature

A digital signature is an electronic signature. It, too, is just like a paper signature, made with a pen or pencil, except that it is fully electronic. However, a digital is impossible to forge, making it more secure than a paper signature or other types of electronic signatures.

A digital signature is restricted to a mathematically encrypted signature through use of cryptography. An example of a digital signature would be where an electronic form is signed, through use of a public key infrastructure. Changes made to this form after it is signed are detected by the engines of the cryptography. The recipient of the form will be notified that the contents of the form have changed and that the digital signature may not be valid or trustworthy. A valid digital signature provides a guarantee to a recipient that the signed file came from a person who sent it and that it was not altered since it was digitally signed.

Digital signatures are a large part of securing electronic information, along with encryption. These technologies combine addresses and solve security issues of

"confidentiality," "integrity," "authentication," "non-repudiation" and "access control."

Digital Signature Requirements

From a technical perspective, the following requirements exist for enabling digital signature technology:

- A public key infrastructure (PKI)
- Enables public and private keys which allow digital signatures to be secure
- Contains certificates to hold the public keys
- Contains a certificate authority (CA) to generate, revoke, etc. certificates
- Contains a registration authority (RA) to command the CA -- to authorize certificate handling.
- A profile, smart card or other device to securely maintain the private keys
- Electronic applications (enabled by the PKI) to which digital signatures can be applied (i.e. electronic forms, e-mail, etc.)
- A Directory to store the certificates and lists of revoked certificates (CRL's)

Electronic Signatures

The definition of an electronic signature is very broad. An electronic signature is just like a paper signature, made with a pen or pencil, except that it is fully electronic. Depending on the type of electronic signature used, there may not be a way to guarantee that an electronic signature is valid. No guarantee can be made because electronic signatures encompass signatures with "electronic pens"; meaning, there is no way to prove that the person is who they say they are based on the signature alone. For example, when making credit card purchases while shopping, someone other than the owner of the signature could forge the signature and make a purchase

Electronic signatures may also be made on personal computers for E-commerce or created in a public key infrastructure environment. The latter is known as a "digital signature."

Encrypted Message

An encrypted message can be created by performing a high processing mathematical function. This function converts every character in that message into some other character.

This mathematical function can be performed using a symmetric key. Since this key is not private, the main challenge with an encrypted message is secure delivery of this

symmetric key to its final destination. This is accomplished by performing encryption on the symmetric key using the recipient's public key.

At this point, an encrypted message has been created.

Encryption

To "encrypt" a file is to apply a mathematical function that transforms every character in the file into some other character. Encryption renders the file unreadable. This means no one, including you, can read the file until it is "decrypted," or conformed back into the original characters. Only the generator of the file and the authorized recipients can decrypt the file.

Hash Function

The process of digital signing can begin by taking a mathematical summary of the document. This is known as a "hash code." This hash code is a uniquely identifying digital fingerprint of the document or message. If the message changes even by one bit, the hash code will dramatically change.

The hash code is then signed with the creator's private key, locking it until the recipient of the message opens it.

At this point, a digitally signed message has been created.

The recipient of the message can verify that the digital signature applied to it is actually from the creator and not an imposter. This is accomplished using the creator's public key. The original hash code is "unlocked" using this public key. Next, a new hash code is created and compared to the original. If these two hash codes match, the digital signature is valid.

A hash function is an algorithm mapping or translation of one sequence of bits into another generally smaller set such that:

a. A message yields the same hash result every time the algorithm is executed using the same message as input,
b. It is computationally infeasible that a message can be derived or reconstituted from the hash result produced by the algorithm, and
c. It is computationally infeasible that two messages can be found that produce the same hash result using the algorithm.

Key Pair Generation

With the implementation of a PKI, key pairs are generated as follows:

Public Keys

Public keys are generated when certificates are issued by the Certificate Authority. (through instruction by the Registration Authority). Public keys are an entry in the user's certificate, which is stored in the Directory. These keys are accessible to recipients of messages from the user who need to unlock or decrypt encrypted messages or verify digitally signed messages sent by that user.

Private Keys

Private keys are generated with the creation of the user's profile. The user is set up by the Registration Authority and then chooses a password, according to agency password rules (i.e. no dictionary words, must have at least one capital letter, must have at least one number, must be at least 8 characters, etc.). Once the user generates this password, his/her profile is created automatically, which contains the private key. Private keys are held by the user only to maintain non-repudiation. Only the user has access to this private key, stored securely in the profile on the user's desktop, smartcard or other device.

Only the recipient has the corresponding private key (corresponding to the public key which encrypted the symmetric key) for unlocking the symmetric key, so only the intended recipient will be able to decrypt the message and read it.

Non-Repudiation

Strong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents.

Privacy

The ability of an individual or organization to control the collection, storage, sharing, and dissemination of personal and organizational information.

Public Key Cryptography

The primary feature of public key cryptography is that it removes the need to use the same key for encryption and decryption of information. With public key cryptography, keys come in matched pairs of "public" and "private" keys. The public portion of the key pair can be distributed in a public manner without compromising the private portion, which must be kept secret by its owner. An encryption operation done with a public key can only be undone with the corresponding private key. Prior to the

invention of public key cryptography, it was essentially impossible to provide key management for large-scale networks. For example, a network of 100 users would require almost 5,000 keys if it used the prior technology, symmetric cryptography. Doubling such a network to 200 users increases the number of keys to almost 20,000.

Although not a total comprehensive solution to key management problems, the invention of public key cryptography was of central importance to the field of cryptography and provided answers to many key management problems for large-scale networks.

Public Key Infrastructure (PKI)

The comprehensive system required to provide public-key encryption and digital signature services is known as a *public-key infrastructure* (PKI). The purpose of a public-key infrastructure is to manage keys and certificates. By managing keys and certificates through a PKI, an organization establishes and maintains a trustworthy networking environment. A PKI enables the use of encryption and digital signature services across a wide variety of applications.

Registration Authority

The registration authority refers to the people, processes and tools used to support the registration of users with the PKI (enrollment) and ongoing administration of users. The certificate authority relies on the Registration Authority for instruction.

Signed Message

A signed message is created by applying a digital signature (electronic signature) to a document/message; like word processing, electronic mail or an electronic form in lieu of a paper signature.

Time-stamp

a. To create a notation that indicates, at least, the correct date and time of an action, and the identity of the person that created the notation; or

b. Such a notation appended, attached, or referenced.

IX. PKI and Digital Signature Standards

As the Commonwealth adopts a PKI strategy and begins to reengineer its business practices, it should ensure that industry standards are being adhered to as much as possible to reduce the risk of non-standard implementations and to take advantage of economies of scale. The following table addresses the various industry standards, their definitions, and how and when they should be used in a PKI. Standards are still evolving, particularly with respect to technical interoperability. They are, however, adequately stable at this time not to present an obstacle to action.

Virginia Information Providers Network,
Glossary of Digital Signature Standards, Protocols, & Terms

Encryption

Abbr.	Full Name	Explanation	Comments	Reference
DES	Data Encryption Standard	Symmetric encryption system (first developed by IBM, and became standard in 1981). Until recently it has been considered secure, but now the technology has reached the point when finding a stronger algorithm is required. Enen, the so-called Triple-DES has been found to be vulnerable to brute force attacks. Advanced Encryption Standard is the industry project aimed at selecting such an algorithm to become a new symmetric encryption standard.	AES development should be monitored, and solutions should allow for an upgrade to the new standard.	US FIPS Pub46-2 and ANSI X3.92 and ANSI X9.52
CAST		Devised by Northern Telecom. Symmetric cryptographic algorithm. Good for large blocks of data. Similar in function to DES. Used by several applications.		Internet RFC 2144
RC2		RSA symmetric encryption algorithm. Also RC4 and RC5.	Internet Draft "A Description of the RC2 Encryption Algorithm"	Internet Draft R. Rivest 6/24/97

Digital Signatures

Abbr	Full Name	Explanation	Comments	Reference
DSS	US Digital Signature Standard	It defines the Digital Signature Algorithm	All solutions must support this standard	
DSA	Digital Signature Algorithm	This is the algorithm for digital signatures based on *discrete logarithm problem for finite fields* (as opposed to RSA or elliptic curve discrete logarithm problem). It can only be used for signatures, not for encryption (which means that US government export restrictions don't apply to it). It is quite computation intensive (longer signature processing time)	All solutions must include this algorithm since it is widely used	US FIPS Pub 186 and ANSI X9.30
RSA Encryption	Rivest-Shamir-Adleman Encryption algorithm	This is the most important public key encryption algorithm. It can be used for encryption and digital signatures. Its strength (depending on the key length) is a subject of US government export restrictions. When used for digital signatures, it is faster than DSA, but more computationally intensive than ECDSA.	All solutions must support this algorithm.	PKCS#1
ECDSA	Elliptic Curve Digital Signature Algorithm	Standard for digital signature algorithm using the *discrete logarithm problem for elliptic curve*. Conceptually it is similar to DSA, as it can't be used for encryption. It is very efficient, as it requires the smallest key lengths (hence it can be used with small devices, as smart cards or tokens). The standard is being developed by IEEE and ANSI. The developments in this area should be monitored, as the knowledge of elliptic curve cryptosystems (which may have profound effects on the algorithm) has been increasing rapidly in recent years.	All solutions must support this algorithm	
PKCS	Public Key	Standards for public key	All solutions must	

	Cryptography Standards	cryptography. (It is being developed by RSA Data Security Inc.) The standard consists of sets of specifications of which the most relevant are: PKCS#4 (now incorporated in PKCS#1): RSA Encryption Standard, PKCS#7:specifies a general format for cryptographic messages, PKCS#10: certificate request standard PKCS#11: cryptographic token interface standard PKCS#12: specifies a portable format for storing or transporting a user's private keys, certificates, miscellaneous secrets, etc.	comply with these standards	
SHA-1	Secure Hash Algorithm	Hash function		US FIPS Pub 180-1 and ANSI X9.30
MD5	Message Digest Algorithm	Hash function		Internet RFC 1321

Terms/Formats/Protocols

Abbr	Full Name	Explanation	Comments	Reference
PKI	Public Key Infrastructures	Infrastructures comprised of supporting services needed for wide scale use of public key technology for secure information exchange. These should satisfy the following requirements: *scalability*: ability to multiply the size of population throughout which the public-key technology can be employed *support for multiple applications* such as e-mail programs, Web transactions, file transfers *interoperability of separately administered infrastructures* it	This is a broad, general description	

		should be possible to integrate infrastructures which are separately administered (e.g. via a LDAP directory services) *support multiple policies*: different certification policies may be required for different applications and users *simple and reliable risk management*: understand risks inherent in public key solutions and know how to minimize them. *limitation of certification authority liability:* liability should be apportioned and limited to discernable risks, e.g. CA should not be responsible for protecting the users private keys, and should not be liable for damages resulting from improper uses of certificates as in the case of compromised private keys. *standards* appropriate standards (technical and legal) should be established and applied.		
PKIX (working group)	Internet Engineering Task Force (IETF) Public-Key Infrastructure Working Group	Working group setting restrictions on the use of fields in X.509 certificates, thus defining PKIX X.509 certificate profile.	One of the more important groups working on PKI standards.	
PKIX (profile)	Internet Public Key Infrastructure Profile	One of X.509 certificate profiles defined by the PKIX working group. X.509 specification differs from an X.509 profile, as it sets limitations on what can or can't appear on a certificate compliant with X.509 standard. Other examples of X.509 profiles are: FPKI (US Federal Gov. PKI profile, MISSI (US DoD profile).	It is important to remember that in practice one deals not just with X.509 certificates, but with specific X.509 profiles for certificates, which may differ depending on the group that defines a given profile. PKIX is one of the	

			most important groups, so all solutions should support this certificate profile.	
X.509 v.3	X.509 version 3 certificate format	This is the current standard for certificates for certifying public keys. The standard (based on X.500 directory standard, but is not limited to X.500's naming system) specifies the information to be contained in a certificate; *Mandatory information:* Version (of Certificate Format), Certificate Serial Number, Signature Algorithm Identifier (for Certificate Issuer's Signature), Issuer (Certificate Authority) X.500 Name, Validity Period (Start and Expiration Dates/Times), Subject X.500 Name, Subject Public Key Info. (Algorithm Identifier, Public Key Value), CA Digital Signature *Optional Info.:* Issuer Unique Identifier, Subject Unique Identifier, Extensions (in the format: Ext. Type, Crit./Non-crit., Extension Field Value)	This is the format of certificates that states will be using. All solutions must support this format of certificates	
X.509 CRL	X.509 Certificate Revocation List standard (for	This is a data structure (maintained by a CA) for providing notices about revocation of certificates. It is a time-stamped list of revoked certificates that were signed by the CA and made available to users. The CRL concept is a part of X.509 standard (X.509 defines the format for a CRL entry). In CRL each certificate is identified by its unique serial number. A certificate should be able to confirm that a given certificate is not on a 'suitably recent' (suitably is defined by PKI policy) CRL. CA issues	CRLs are critical to PKI integrity, so solutions must include CRLs available to the users via retrieving or broadcasting.	

		CRLs periodically (hourly, daily, or weekly - again this is subject to PKI policy). CRLs may be retrieved by users of the PKI, or delivered to the users as soon as they change. (Both systems of making CRL available have advantages and problems)		
OCSP	Online Certificate Status Protocol	Protocol designed for checking the revocation status of the certificates. From specs: The Online Certificate Status Protocol (OCSP) enables applications to determine the (revocation) state of an identified certificate. OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and may also be used to obtain additional status information. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate in question until the responder provides a response.	Incorporation of OCSP servers and clients may be a solution for verifying revocation status of certificates	
CA	Certification Authority	An organization issuing digital certificates for public/private keys. (used by individuals, organizations, other CAs, servers, computer programs, etc.)	A PKI will include a number of CAs (which may be chained in some way). May also admit established CAs (e.g. VeriSign, Entrust, XCert, etc) to play a role in a PKI.	
CPS	Certification Practice Statement	Statement of practices that a certification authority employs in issuing certificates (as defined in ABA Dig. Sign. Guidelines. It should include: *a clear and complete articulation of the parties' legal rights and*	States will have to formulate their CPS(s), which may vary from state to state, depending on local laws	

		obligations, *A systematic description of pertinent aspects of the operational environment and encapsulation of current industry knowledge and accepted practices.* CPS may be a declaration by the CA, or become a part of the contract between the CA and the subscriber. The terms fundamental to certification practices are: issuing authority (CA), nonverified subscriber information (information submitted by the subscriber to be included in a certificate, but not verified by the CA), operation period of a certificate, certificate user (relying party), repository of certificates, subscriber (party being the subject of the certificate)		
LRA	Local Registration Authority	Trusted persons appointed by the CA to assist subscribers in applying for certificates; they may be very useful in the critical process of verification of the information to be certified by the CA.	States may need LRAs as a service to subscribers.	
LDAP	Lightweight Directory Access Protocol	A protocol (developed by Netscape) for accessing information stored in a directory based on X.500 directory model. In general, a directory service consists of a system of database servers and clients using a specific protocol for passing the data between themselves and for accessing and updating the data. The directory databases store many small pieces of attribute-based information (e.g. personal data, certificates, application configuration files). The information is mostly read from	States will need to have a directory service to manage the PKI certificate life cycle and distribute and locate certificates. States may also find it useful to store application configuration files in a directory. LDAP based directory service seems to be essential to a	

		and rarely written to the directory database. Directory has to have search and browsing capabilities. Very important (for reliability and fast access) is replication of the directory data in a system of replica directory servers.	robust PKI.	

X. Chapter Notes

II. Introduction

1. Whitter.
2. Governor's Commission on Information Technology.
3. Whitter.
4. Zimits and Montano.
5. Ibid.
6. Ibid.
7. Whitter.

III. Electronic Signatures and their Components

1. National Conference of Commissioners on Uniform state Laws.
2. American Bar Association.
3. Govt. Paperwork Elimination Act.
4. VA Internet Policy
5. Entrust.
6. Ibid.
7. Curry, "Trusted PKI."
8. Zimits and Montano.
9. Ibid.
10. Ibid.
11. Ibid.
12. Ibid.
13. Ibid.
14. Entrust.
15. Whitter.
16. Zimits and Montano.

IV. Legal Frameworks

1. American Bar Association
2. Governor's Commission on Information Technology.

Findings and Recommendations

1. Zimits and Montano.
2. Ibid.

XI. Works Cited

American Bar Association, Information Security Committee Science and Technology Section, “Digital Signature Guidelines”, Aug 1996.

Commonwealth of Virginia, “Virginia’s Internet Policy and Secretariat of Technology”, 1999 Edition.

Curry, Ian, “The Concept of Trust in Network Security”, Entrust technologies, Dec 1995.

Curry, Ian, “Trusted Public-Key Infrastructures”, Entrust Technologies, Dec 1997.

Entrust, “Virginia PKI Glossary Terms”, Entrust Technologies, Oct 1999.

Government Paperwork Elimination Act (GPEA) as part of H.R. 4328, the Fiscal 1999 Omnibus Appropriations Act, Oct 1998.

Governor’s Commission on Information Technology, “Toward a Comprehensive Internet Policy for the Commonwealth of Virginia”, Dec 1998.

Government Information Technology Services Board, “Access with Trust”, Federal PKI Steering Committee, Sept 1998.

National Conference of Commissioners on Uniform state Laws, “Uniform Electronic Transactions Act,” Jul 1999.

Treasury Board of Canada Secretariat, “Policy for Public Key Infrastructure Management in the Government of Canada”, May 1999.

Whitter, Jim, “Policies Concerning the Acceptance of Electronic Signatures: States Take the Lead”, Natural Resources Policy Studies Division, NGA Center for Best Practices, Apr 1999.

Zimits and Montano, “Public Key Infrastructure: Unlocking the Internet's Economic Potential”, Hambrecht & Quist LLC., Apr 1998.